A NEW UPPER BOUND FOR THE CROSS NUMBER OF FINITE ABELIAN GROUPS

by

Benjamin Girard

Abstract. — In this paper, building among others on earlier works by U. Krause and C. Zahlten (dealing with the case of cyclic groups), we obtain a new upper bound for the little cross number valid in the general case of arbitrary finite Abelian groups. Given a finite Abelian group, this upper bound appears to depend only on the rank and on the number of distinct prime divisors of the exponent. The main theorem of this paper allows us, among other consequences, to prove that a classical conjecture concerning the cross and little cross numbers of finite Abelian groups holds asymptotically in at least two different directions.

1. Introduction

Let G be a finite Abelian group, written additively. By $\mathrm{r}(G)$ and $\exp(G)$ we denote respectively the rank and the exponent of G. If G is cyclic of order n, it will be denoted by C_n. In the general case, we can decompose G (see for instance [27]) as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ where $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, so that every element g of G can be written $g = [a_1, \ldots, a_r]$ (this notation will be used freely along this paper), with $a_i \in C_{n_i}$ for all $i \in [\![1, r]\!] = \{1, \ldots, r\}$.

In this paper, any finite sequence $S = (g_1, \ldots, g_l)$ of l elements from G will be called a *sequence* of G with *length* l. Given a sequence $S = (g_1, \ldots, g_l)$ of G, we say that $s \in G$ is a *subsum* of S when it lies in the following set, called the *sumset* of S:

$$\Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \subsetneq I \subseteq \{1, \ldots, l\} \right\}.$$

If 0 is not a subsum of S, we say that S is a *zero-sumfree sequence*. If $\sum_{i=1}^{l} g_i = 0$, then S is said to be a *zero-sum sequence*. If moreover one has $\sum_{i \in I} g_i \neq 0$ for all proper subsets $\emptyset \subsetneq I \subsetneq \{1, \ldots, l\}$, S is called a *minimal zero-sum sequence*.

In a finite Abelian group G, the order of an element g will be written $\mathrm{ord}(g)$ and for every divisor d of the exponent of G, we denote by G_d the subgroup of G consisting of all the elements of order dividing d:

$$G_d = \{x \in G \mid dx = 0\}.$$

Mathematics Subject Classification (2000): 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05.

B. GIRARD, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France (*e-mail*: benjamin.girard@math.polytechnique.fr).

In a sequence S of elements of G, we denote by S_d the subsequence of S consisting of all the elements of order d contained in S.

Let $\mathcal{P} = \{p_1 = 2 < p_2 = 3 < \dots\}$ be the set of prime numbers. Given a positive integer $n \in \mathbb{N}^* = \mathbb{N}\backslash\{0\}$, we denote by $\mathcal{D}_n$ the set of its positive divisors. If $n > 1$, we denote by $P^-(n)$ the smallest prime element of $\mathcal{D}_n$, and we put by convention $P^-(1) = 1$. By $\tau(n)$ and $\omega(n)$ we denote respectively the number of positive divisors of n and the number of distinct prime divisors of n.

By $\mathsf{D}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a zero-sum subsequence. The constant $\mathsf{D}(G)$ is called the *Davenport constant* of the group G.

By $\eta(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G with length $|S| \geq t$ contains a zero-sum subsequence $S' \subseteq S$ with length $|S'| \leq \exp(G)$. Such a subsequence is called a *short zero-sum subsequence*.

The constants $\mathsf{D}(.)$ and $\eta(.)$ have been extensively studied during last decades and even if numerous results were proved (see Chapter 5 of the book [13] or [9] for a survey and many references on the subject), their exact values are known for very special types of groups only. In the sequel, we shall need some results on some of the groups for which we know the exact values, so we gather what is known concerning them in the following theorem.

Theorem 1.1. — *The two following statements hold:*

(*i*) *Let $p \in \mathcal{P}$, $r \in \mathbb{N}^*$ and $\alpha_1 \leq \dots \leq \alpha_r$, where $\alpha_i \in \mathbb{N}^*$ for all $i \in [\![1, r]\!]$. Then, for the p-group $G \simeq C_{p^{\alpha_1}} \oplus \dots \oplus C_{p^{\alpha_r}}$, we have:*

$$\mathsf{D}(G) = \sum_{i=1}^{r} (p^{\alpha_i} - 1) + 1.$$

(*ii*) *For every $m, n \in \mathbb{N}^*$ with $m|n$, we have:*

$$\mathsf{D}(C_m \oplus C_n) = m + n - 1 \quad \textit{and} \quad \eta(C_m \oplus C_n) = 2m + n - 2.$$

In particular, we have $\mathsf{D}(C_n) = \eta(C_n) = n$.

Proof. — (*i*) This result was proved by J. Olson in [21] using the notion of group algebra. The special case of elementary p-groups, which says that $\mathsf{D}(C_p^r) = r(p-1)+1$, can be easily deduced from the Chevalley-Warning theorem (see [7] for example).

(*ii*) The value of $\mathsf{D}(.)$ for groups with rank 2 is also due to J. Olson (see [22]), and uses the special case $\eta(C_p^2) = 3p - 2$ with p prime. The complete statement for $\eta(.)$ has been proved by A. Geroldinger and F. Halter-Koch (see [13], Theorem 5.8.3).

□

The value of $\eta(.)$ for Abelian p-groups with rank $r \geq 3$ is not known in general, even in the special case of elementary p-groups. It is only known that for every $r \in \mathbb{N}^*$, we have $\eta(C_2^r) = 2^r$, and it is conjectured that for every odd $p \in \mathcal{P}$, we have $\eta(C_p^3) = 8p - 7$ and $\eta(C_p^4) = 19p - 18$. The interested reader is for instance referred to [5] and [10], for a complete account on this topic.

Yet, N. Alon and M. Dubiner showed in [1] an important theorem related to the constant $\eta(.)$ of elementary p-groups. We will use the following corollary of this result.

Theorem 1.2. — *For every $r \in \mathbb{N}^*$, there exists a constant $c_r > 0$ such that for every $p \in \mathcal{P}$, the following holds:*

$$\eta\left(C_p^r\right) \leq c_r(p-1)+1.$$

In this paper, we will study the *cross number* of finite Abelian groups. For this purpose, we recall some definitions and also the results known so far, to the best of our knowledge, concerning this constant. Let G be a finite Abelian group. If $G \simeq C_{\nu_1} \oplus \cdots \oplus C_{\nu_s}$, with $\nu_i > 1$ for all $i \in [\![1, s]\!]$, is the longest possible decomposition of G into a direct product of cyclic groups, then we set:

$$\mathsf{k}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i},$$

and

$$\mathsf{K}^*(G) = \sum_{i=1}^{s} \frac{\nu_i - 1}{\nu_i} + \frac{1}{\exp(G)} = \mathsf{k}^*(G) + \frac{1}{\exp(G)}.$$

The *cross number* of a sequence $S = (g_1, \ldots, g_l)$, denoted by $\mathsf{k}(S)$, is defined by:

$$\mathsf{k}(S) = \sum_{i=1}^{l} \frac{1}{\operatorname{ord}(g_i)}.$$

Then, we define the *little cross number* $\mathsf{k}(G)$ of G:

$$\mathsf{k}(G) = \max\{\mathsf{k}(S) | S \text{ zero-sumfree sequence of } G\},$$

as well as the *cross number* of G, denoted by $\mathsf{K}(G)$:

$$\mathsf{K}(G) = \max\{\mathsf{k}(S) | S \text{ minimal zero-sum sequence of } G\}.$$

The cross number was introduced by U. Krause in [19] in order to clarify the relationship between the arithmetic of a Krull monoid and the properties of its ideal class group. For this reason, the cross number plays a key rôle in the theory of non-unique factorization (see [19], [8], [15], [28], [23], [24] and [25] for some applications of the cross number, the surveys [3], [14] and the book [13] which presents exhaustively the different aspects of the theory).

For the sake of completeness, we mention that the cross number has been studied in other directions also (see for example [4], [18] and [2]), and that this concept arose in a natural way in combinatorial number theory (see for instance [11] and [6]).

Given a finite Abelian group G, a natural construction (see [19] or [13], Proposition 5.1.8) gives the following lower bounds:

$$\mathsf{k}^*(G) \leq \mathsf{k}(G) \quad \text{and} \quad \mathsf{K}^*(G) \leq \mathsf{K}(G),$$

yet, except for Abelian p-groups (see [12]) and other special cases (see [16]), the exact values of the cross and little cross numbers are also unknown in general, even for cyclic groups. In addition, still no counterexample is known for which equality does not hold in the previous inequalities, which would allow us to disprove the following conjecture.

Conjecture 1.3. — *For every finite Abelian group G, one has the following:*

$$\mathsf{k}^*(G) = \mathsf{k}(G) \quad \text{and} \quad \mathsf{K}^*(G) = \mathsf{K}(G).$$

Regarding upper bounds, and since the constants $\mathsf{k}(.)$ and $\mathsf{K}(.)$ are closely related to each other, it suffices, according to the following proposition (see [13], Proposition 5.1.8), to bound from above the little cross number so as to bound from above the cross number, but also the Davenport constant. Since $\mathsf{k}(.)$ is easier to handle, one usually prefers to study the cross number via the little cross number, and we will do so in this paper.

Proposition 1.1. — *Let G be a finite Abelian group with $\exp(G) = n$. Then, the two following statements hold:*

(i)

$$\mathsf{k}(G) + \frac{1}{n} \leq \mathsf{K}(G) \leq \mathsf{k}(G) + \frac{1}{P^-(n)},$$

(ii)

$$\mathsf{D}(G) \leq n\mathsf{k}(G) + 1.$$

Two types of upper bounds are currently known for $\mathsf{k}(.)$. The first one holds for any finite Abelian group, and was obtained by A. Geroldinger and R. Schneider in [17] and in [13], Theorem 5.5.5, using character theory and the notion of group algebra.

Theorem 1.4. — *Let G be a finite Abelian group with $\exp(G) = n$. Then, for every $d \in \mathcal{D}_n$, one has the following:*

$$\mathsf{k}(G) \leq \frac{d-1}{P^-(n)} + \log\left(\frac{|G|}{d}\right).$$

In particular $\mathsf{k}(G) \leq \log|G|$.

Eventhough this upper bound is general and easy to compute, it does not really fit what we know about the behaviour of the cross number. For example, let $r > 1$ be an integer. If we consider an elementary p-group with rank r, it is known that $\mathsf{k}\left(C_p^r\right) = \mathsf{k}^*\left(C_p^r\right) \leq r$, yet $\log\left(|C_p^r|/p\right) = (r-1)\log p$ diverges when p tends to infinity.

From this point of view, and in the special case of cyclic groups, a more precise upper bound was found by U. Krause and C. Zahlten in [20] which, expressed with our notations, gives the following.

Theorem 1.5. — *For every $n \in \mathbb{N}^*$, one has the following:*

$$\mathsf{k}(C_n) \leq 2\omega(n).$$

It should be underlined that this upper bound has the right order of magnitude, since one has $\mathsf{k}(C_n) \geq \mathsf{k}^*(C_n) \geq \omega(n)/2$ by definition.

2. New results and plan of the paper

In this paper, we generalize the work of [20] to every finite Abelian group so as to obtain a new upper bound for the little cross number in the general case, which no longer depends on the cardinality of the group considered, and which supports the conjecture that the little cross number of a finite Abelian group G with rank r and exponent n is less than $r\omega(n)$.

For this purpose, we introduce the two following constants. Let G be a finite Abelian group and $d', d \in \mathbb{N}^*$ be two integers such that $d \in \mathcal{D}_{\exp(G)}$ and $d' \in \mathcal{D}_d$.

By $\mathsf{D}_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence of sum in $G_{d/d'}$.

By $\eta_{(d',d)}(G)$ we denote the smallest integer $t \in \mathbb{N}^*$ such that every sequence S of G_d with length $|S| \geq t$ contains a subsequence $S' \subseteq S$ of length $|S'| \leq d'$ and of sum in $G_{d/d'}$.

To start with, we will prove in Section 3 (Proposition 3.1), that for any finite Abelian group G and every $1 \leq d' \mid d \mid \exp(G)$, $\mathsf{D}_{(d',d)}(G)$ and $\eta_{(d',d)}(G)$ are linked to the constants $\mathsf{D}(.)$ and $\eta(.)$ of a particular subgroup $G_{\upsilon(d',d)}$ of G.

In Section 4, we will prove the main theorem (Theorem 2.1). This result will be stated at the end of this section. Before giving this general and technical theorem, we emphasize the many consequences it has.

To obtain these results, we introduce the two following arithmetic functions:

$$\alpha(n) = \sum_{d \in \mathcal{D}_n} \frac{P^-(d) - 1}{d} \quad \text{and} \quad \beta(n) = \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{P^-(d) - 1}{d},$$

which will be investigated in Section 5. In particular, simple upper bounds for these functions lead, by applying the main theorem, to the following qualitative result, proved in Section 6.

Proposition 2.1. — *For every $r \in \mathbb{N}^*$ there exists a constant $d_r > 0$ such that, for every finite Abelian group G with $r(G) \leq r$ and $\exp(G) = n$, the following holds:*

$$\mathsf{k}(G) \leq d_r \omega(n).$$

Consequently, when considering the cross number of a finite Abelian group G with fixed or bounded rank, Proposition 2.1 gives a qualitative upper bound which depends only on the number of distinct prime divisors $\omega(n)$ of $\exp(G) = n$, and which improves, at least asymptotically, the one stated in Theorem 1.4, since the function ω can have arbitrary small values in $\mathbb{N}^*$ even for arbitrary large n, but mainly since it is known (see for instance Chapter I.5 of the book [30]) that one has:

$$\omega(n) \lesssim \frac{\log n}{\log \log n}.$$

In addition, more accurate upper bounds for some sequences built with $\alpha(n)$ and $\beta(n)$, obtained in Lemma 5.1 (see Section 5), enable us to prove the following quantitative result (see Section 6) which states that when $r = 1$ or 2, one can choose d_r in the following way:

$$d_1 = \frac{166822111}{109486080} \approx 1.5237 \qquad \text{and} \qquad d_2 = \frac{1784073894563}{476759162880} \approx 3.7421.$$

Once d_1 and d_2 are defined in such a way, one can state the following proposition.

Proposition 2.2. — *(i) For every cyclic group $G \simeq C_n$, $n \in \mathbb{N}^*$, we have:*

$$\mathsf{k}(G) \leq \alpha(n) \leq d_1\omega(n).$$

(ii) For every finite Abelian group $G \simeq C_m \oplus C_n$, with $1 < m \mid n \in \mathbb{N}^*$, we have:

$$\mathsf{k}(G) \leq 3\alpha(n) - \beta(n) \leq d_2\omega(n).$$

Moreover, the asymptotical behaviours of $\alpha(n)$ and $\beta(n)$, studied in Lemma 5.2, imply several asymptotical results, some of them being sharp, concerning the cross and little cross numbers as well as the Davenport constant. In particular, these results show that Conjecture 1.3 holds asymptotically in at least two different directions. These results will be proved in Section 7, and in order to state them, we will need the following notation. For every $r \in \mathbb{N}^*$ and $l_1, \dots, l_r \in \mathbb{N}^*$, we set:

$$\mathcal{E}_{(l_1,\dots,l_r)} = \left\{ \bigoplus_{i=1}^{r} C_{n_i},\ 1 < n_1 | \dots | n_r \in \mathbb{N} \mid \forall i \in [\![1, r]\!],\ \omega(n_i) = l_i \text{ and } \gcd\left(n_i, \frac{n_r}{n_i}\right) = 1 \right\}.$$

Proposition 2.3. — *For every $r \in \mathbb{N}^*$ and $l_1, \dots, l_r \in \mathbb{N}^*$, the following statements hold:*

(i)

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\dots,l_r)}}} \mathsf{k}(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

(ii)

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\dots,l_r)}}} \mathsf{K}(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

(iii)

$$\limsup_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\dots,l_r)}}} \frac{\mathsf{D}(C_{n_1} \oplus \cdots \oplus C_{n_r})}{n_r} \leq \sum_{i=1}^{r} l_i.$$

Concerning the groups of the form C_n^r, we obtain the following corollary by specifying $n_1 = \cdots = n_r$ in Proposition 2.3.

Proposition 2.4. — *For all integers $r, l \in \mathbb{N}^*$ the three following statements hold:*

(i)

$$\lim_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \mathsf{k}(C_n^r) = rl,$$

(ii)

$$\lim_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \mathsf{K}(C_n^r) = rl,$$

(iii)

$$\limsup_{\substack{P^-(n) \to +\infty \\ \omega(n) = l}} \frac{\mathsf{D}(C_n^r)}{n} \leq rl.$$

It may be observed that Proposition 2.3 and Proposition 2.4 are somehow reminiscent of [17], Theorem 2(b), since this result and our Proposition 2.3 give the value of the cross number of "large" groups. However, a more precise look at both results shows that they are of a different nature. Indeed, while A. Geroldinger and R. Schneider's result is not asymptotical but valid only for special groups satisfying some restrictive conditions, ours, although of asymptotical nature, is valid in a wider framework.

The following proposition will also be proved in Section 7.

Proposition 2.5. — *For all $r \in \mathbb{N}^*$, the two following statements hold:*

(*i*)

$$\lim_{\omega(n) \to +\infty} \frac{\mathsf{k}(C_n^r)}{\omega(n)} = r,$$

(*ii*)

$$\lim_{\omega(n) \to +\infty} \frac{\mathsf{K}(C_n^r)}{\omega(n)} = r.$$

All these results are deduced from the following proposition, proved in Section 6 under the stronger form of Proposition 6.1, and which is a somewhat rough corollary of the main theorem (Theorem 2.1). For the sake of clarity, we recall that the constant c_r is the one which has been introduced in Theorem 1.2.

Proposition 2.6. — *Let G be a finite Abelian group with $r(G) = r$ and $\exp(G) = n$. We set $H = C_n^r$ and also:*

$$\varphi(G, H) = \begin{cases} \mathsf{k}^*(H/G) & \text{if } G \text{ is a direct summand of } H, \\ \mathsf{k}^*(H/G)/n & \text{otherwise.} \end{cases}$$

Then, one has the following upper bound for the little cross number $\mathsf{k}(G)$:

$$\mathsf{k}(G) \leq c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n) - \varphi(G, H).$$

The main theorem of this paper (Theorem 2.1) will be proved in Section 4. In order to state it, we will need the following definitions and notations which will be extensively used in Sections 3 and 4.

Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group with $\exp(G) = n$, $\tau(n) = m$ and $d', d \in \mathbb{N}^*$ be such that $d \in \mathcal{D}_n$ and $d' \in \mathcal{D}_d$. For all $i \in [\![1, r]\!]$, we set:

$$A_i = \gcd(d', n_i), \;\; B_i = \frac{\text{lcm}(d, n_i)}{\text{lcm}(d', n_i)},$$

$$\upsilon_i(d', d) = \frac{A_i}{\gcd(A_i, B_i)},$$

and

$$G_{\upsilon(d',d)} = C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}.$$

Then, for every $d \in \mathcal{D}_n = \{d_1, \ldots, d_m\}$ and $x = (x_{d_1}, \ldots, x_{d_m}) \in \mathbb{N}^m$, we set:

$$f_d(x) = \min_{d' \in \mathcal{D}_d \setminus \{1\}} \big(\eta(G_{\upsilon(d',d)})\big) - 1 - x_d,$$

$$g_d(x) = \mathsf{D}(G_{\upsilon(d,d)}) - 1 - \sum_{d' \in \mathcal{D}_d} x_{d'},$$

and

$$h(x) = \sum_{d \in \mathcal{D}_n} \frac{x_d}{d} - \mathsf{k}^*(G).$$

We can now state the main theorem.

Theorem 2.1. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group with $\exp(G) = n$ and $\tau(n) = m$. For every zero-sumfree sequence S of G reaching the maximum $\mathsf{k}(S) = \mathsf{k}(G)$, and being of minimal length regarding this property, the m-tuple $x = (|S_{d_1}|, \ldots, |S_{d_m}|)$ is an element of the polytope $\mathbb{P}_G \cap \mathbb{H}_G$ where:*

$$\mathbb{P}_G = \{x \in \mathbb{N}^m \mid f_d(x) \geq 0,\ g_d(x) \geq 0,\ d \in \mathcal{D}_n\},$$

and

$$\mathbb{H}_G = \{x \in \mathbb{N}^m \mid h(x) \geq 0\}.$$

Keeping the notations of Theorem 2.1, we obtain the following immediate corollary, which gives a general upper bound for the little cross number of a finite Abelian group, expressed as the solution of an integer linear program.

Corollary 2.2. — *For every finite Abelian group G, one has the following upper bound:*

$$\mathsf{k}(G) \leq \max_{x \in \mathbb{P}_G} \left(\sum_{i=1}^{m} \frac{x_{d_i}}{d_i} \right).$$

In principle, the wide generality of Theorem 2.1 and Corollary 2.2 leaves a good hope that it could lead to new - and maybe optimal - upper bounds for $\mathsf{k}(G)$ in the general case. However, such improvements will require a precise study of the polytope $\mathbb{P}_G$, which is certainly a complicated, but not hopeless, task.

3. On the quantities $\mathsf{D}_{(d',d)}(G)$ and $\eta_{(d',d)}(G)$

In this section, we will denote by π_i, for all $i \in [\![1, r]\!]$, the canonical epimorphism from C_{n_i} to $C_{\upsilon_i(d',d)}$. Although this epimorphism clearly depends on d' and d, we do not emphasize this dependence here since there is no risk of ambiguity. Moreover, one can notice that whenever d divides n_i, we have $\upsilon_i(d',d) = \gcd(d', n_i) = d'$, and in particular $\upsilon_r(d',d) = d'$. In the sequel, when $d' = d$, we will write $\upsilon_i(d)$ instead of $\upsilon_i(d,d)$.

Lemma 3.1. — *Let $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$, with $1 < n_1 \mid \ldots \mid n_r \in \mathbb{N}$, be a finite Abelian group and $d', d \in \mathbb{N}^*$ be such that $d \in \mathcal{D}_{\exp(G)}$ and $d' \in \mathcal{D}_d$. Then, for every $g = [a_1, \ldots, a_r] \in G$, we have:*

$$\frac{d}{d'} \left[\frac{n_1}{\gcd(d, n_1)} a_1, \ldots, \frac{n_r}{\gcd(d, n_r)} a_r \right] = 0 \textit{ if and only if } \pi_i(a_i) = 0 \textit{ for all } i \in [\![1, r]\!].$$

Proof. — First, we have the following equalities:

$$\begin{aligned}\frac{d}{d'}\frac{n_i}{\gcd(d,n_i)} &= \frac{\operatorname{lcm}(d,n_i)}{d'}\\ &= \frac{\operatorname{lcm}(d,n_i)n_i}{d'n_i}\\ &= \frac{\operatorname{lcm}(d,n_i)n_i}{\gcd(d',n_i)\operatorname{lcm}(d',n_i)}\\ &= B_i\frac{n_i}{A_i}\in\mathbb{N}.\end{aligned}$$

Let $[a_1,\dots,a_r]\in G$ be such that:

$$\frac{d}{d'}\left[\frac{n_1}{\gcd(d,n_1)}a_1,\dots,\frac{n_r}{\gcd(d,n_r)}a_r\right]=0.$$

For all $i\in[\![1,r]\!]$, one has:

$$\frac{d}{d'}\frac{n_i}{\gcd(d,n_i)}a_i=B_i\frac{n_i}{A_i}a_i=0,$$

which is equivalent, considering a_i as an integer, to the following relation:

$$A_i|B_ia_i,$$

that is to say, dividing each side by $\gcd(A_i,B_i)$, that one has:

$$\upsilon_i(d',d)\ \Big|\ \frac{B_i}{\gcd(A_i,B_i)}a_i,$$

which, since:

$$\gcd\left(\frac{A_i}{\gcd(A_i,B_i)},\frac{B_i}{\gcd(A_i,B_i)}\right)=1,$$

is equivalent to:

$$\upsilon_i(d',d)|a_i,$$

and the desired result is proved. □

Proposition 3.1. — *Let $G\simeq C_{n_1}\oplus\cdots\oplus C_{n_r}$, with $1<n_1\mid\dots\mid n_r\in\mathbb{N}$, be a finite Abelian group and $d',d\in\mathbb{N}^*$ be such that $d\in\mathcal{D}_{\exp(G)}$ and $d'\in\mathcal{D}_d$. Then, we have the two following equalities:*

$$\begin{cases}\mathsf{D}_{(d',d)}(G)=\mathsf{D}\left(C_{\upsilon_1(d',d)}\oplus\cdots\oplus C_{\upsilon_r(d',d)}\right),\\ \eta_{(d',d)}(G)=\eta\left(C_{\upsilon_1(d',d)}\oplus\cdots\oplus C_{\upsilon_r(d',d)}\right).\end{cases}$$

Proof. — Let $[a_1,\dots,a_r]\in G_d$. We know that $\operatorname{ord}([a_1,\dots,a_r])=\operatorname{lcm}(\operatorname{ord}(a_1),\dots,\operatorname{ord}(a_r))$, and so $\operatorname{ord}([a_1,\dots,a_r])\,|d$ implies $\operatorname{ord}(a_i)|d$ for all $i\in[\![1,r]\!]$.

By Lagrange theorem, we also have $\operatorname{ord}(a_i)|n_i$, which implies that:

$$\operatorname{ord}(a_i)|\gcd(d,n_i)\text{ for all }i\in[\![1,r]\!],$$

and since any cyclic group C_{n_i} contains a unique subgroup of order $\gcd(d,n_i)$, we can write:

$$a_i=\frac{n_i}{\gcd(d,n_i)}a'_i\text{ with }a'_i\in C_{n_i}.$$

We now consider a sequence $S = (g_1, \ldots, g_m)$ of G_d with $m \in \mathbb{N}^*$. According to the previous argument, the elements of S have the following form:

$$\begin{array}{ccccc} g_1 & = & [a_{1,1}, \ldots, a_{1,r}] & = & \left[\frac{n_1}{\gcd(d,n_1)} a'_{1,1}, \ldots, \frac{n_r}{\gcd(d,n_r)} a'_{1,r}\right], \\ \vdots & & \vdots & & \vdots \\ g_m & = & [a_{m,1}, \ldots, a_{m,r}] & = & \left[\frac{n_1}{\gcd(d,n_1)} a'_{m,1}, \ldots, \frac{n_r}{\gcd(d,n_r)} a'_{m,r}\right]. \end{array}$$

Let K be a nonempty subset of $\{1, \ldots, m\}$. Then, the sum $\sum_{k \in K} [a_{k,1}, \ldots, a_{k,r}]$ is an element of $G_{d/d'}$ if and only if:

$$\frac{d}{d'} \sum_{k \in K} [a_{k,1}, \ldots, a_{k,r}] = \frac{d}{d'} \left[\frac{n_1}{\gcd(d, n_1)} \sum_{k \in K} a'_{k,1}, \ldots, \frac{n_r}{\gcd(d, n_r)} \sum_{k \in K} a'_{k,r}\right] = 0,$$

and by Lemma 3.1, this relation is equivalent to:

$$\sum_{k \in K} \left[\pi_1(a'_{k,1}), \ldots, \pi_r(a'_{k,r})\right] = 0 \text{ in } \bigoplus_{i=1}^{r} C_{\upsilon_i(d',d)}.$$

Therefore, from the definition of the constant $\mathsf{D}(.)$, one can deduce that the smallest integer $m \in \mathbb{N}^*$ such that for every sequence $S = (g_1, \ldots, g_m)$ of G_d with length $|S| \geq m$, there exists a nonempty subset $K \subseteq \{1, \ldots, m\}$ such that $\sum_{k \in K} [a_{k,1}, \ldots, a_{k,r}]$ is an element of $G_{d/d'}$ is exactly $\mathsf{D}\left(C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}\right)$. This proves the first equality.

If moreover, one expects the additional condition $|K| \leq \upsilon_r(d', d) = d'$ to be verified, then, by the definition of $\eta(.)$, the corresponding smallest possible integer $m \in \mathbb{N}^*$ is exactly $\eta\left(C_{\upsilon_1(d',d)} \oplus \cdots \oplus C_{\upsilon_r(d',d)}\right)$, which proves the second equality. □

4. Proof of the main theorem

Proof of Theorem 2.1. — Let S be a zero-sumfree sequence of G verifying $\mathsf{k}(S) = \mathsf{k}(G)$, and being of minimal length regarding this property. For every $d \in \mathcal{D}_n$, we set $x_d = |S_d|$, and we suppose that the m-tuple $x = (x_{d_1}, \ldots, x_{d_m})$ is not an element of the polytope $\mathbb{P}_G \cap \mathbb{H}_G$. Thus, one has the three following cases.

Case 1. There exists $d_0 \in \mathcal{D}_n$ such that $f_{d_0}(x) < 0$. Therefore, it exists $d'_0 \in \mathcal{D}_{d_0} \backslash \{1\}$ verifying $x_{d_0} \geq \eta\left(C_{\upsilon_1(d'_0,d_0)} \oplus \cdots \oplus C_{\upsilon_r(d'_0,d_0)}\right)$ which means, by Proposition 3.1, that $x_{d_0} \geq \eta_{(d'_0,d_0)}(G)$. So, the sequence S contains X elements of order d_0, with $1 < X \leq d'_0$, the sum of which is an element of order $\tilde{d}_0$ dividing d_0/d'_0.

Let S' be the sequence obtained from S by replacing these X elements by their sum. In particular, we have $|S'| = |S| - X + 1 < |S|$. Moreover, S' is a zero-sumfree sequence and verifies the following equalities:

$$\begin{cases} |S'_{d_0}| = |S_{d_0}| - X, \\ |S'_{\tilde{d}_0}| = |S_{\tilde{d}_0}| + 1, \\ |S'_d| = |S_d| \ \forall d \neq d_0, \tilde{d}_0. \end{cases}$$

Since

$$\frac{1}{\tilde{d_0}} - \frac{X}{d_0} \geq 0,$$

one has the following inequalities:

$$\begin{aligned}
\mathsf{k}(S) &= \sum_{d \in \mathcal{D}_{\exp(G)}} \frac{x_d}{d} \\
&\leq \sum_{d \in \mathcal{D}_{\exp(G)} \setminus \{d_0, \tilde{d_0}\}} \frac{x_d}{d} + \frac{x_{\tilde{d_0}} + 1}{\tilde{d_0}} + \frac{x_{d_0} - X}{d_0} \\
&= \mathsf{k}(S').
\end{aligned}$$

So, we obtain $\mathsf{k}(S') = \mathsf{k}(G)$ and $|S'| < |S|$, which is a contradiction.

Case 2. There exists $d_0 \in \mathcal{D}_n$ such that $g_{d_0}(x) < 0$. As a consequence, we have $\sum_{d \in \mathcal{D}_{d_0}} x_d \geq \mathsf{D}(C_{\upsilon_1(d_0)} \oplus \cdots \oplus C_{\upsilon_r(d_0)})$ and Proposition 3.1 gives the existence of a zero-sum subsequence, which is a contradiction.

Case 3. One has $h(x) < 0$, that is to say $\mathsf{k}(S) = \mathsf{k}(G) < \mathsf{k}^*(G)$ which is a contradiction. $\square$

An interesting special case is the one of finite Abelian groups with rank 2. Indeed, for such groups, all the parameters used to define the polytope $\mathbb{P}_G$ in the main theorem are known by Theorem 1.1:

$$\mathsf{D}_{(d,d)}(G) = \upsilon_1(d) + \upsilon_2(d) - 1 \quad \text{and} \quad \eta_{(d',d)}(G) = 2\upsilon_1(d', d) + \upsilon_2(d', d) - 2,$$

and therefore allow us to compute an explicit upper bound for the little cross number $\mathsf{k}(G)$ by linear programming methods (see for instance the book [29] for an exhaustive presentation of these methods).

5. Some sequences related to the exponent of a finite Abelian group

Let $(\alpha_l)_{l \geq 1}$ and $(\beta_l)_{l \geq 1}$ be the two following sequences of integers, built from the set of prime numbers:

$$\alpha_1 = 1 \text{ and } \alpha_l = 1 + \frac{p_l}{p_l - 1}\alpha_{l-1} \text{ for all } l \geq 2,$$

as well as

$$\beta_l = \sum_{i=1}^{l} \frac{p_i - 1}{p_i} \text{ for all } l \geq 1.$$

Finally, we define a third sequence $(\gamma_l)_{l \geq 1}$ in the following fashion:

$$\gamma_l = 3\alpha_l - \beta_l \text{ for all } l \geq 1.$$

The first values of $(\alpha_l)_{l \geq 1}$ are the following:

$$\alpha_1 = 1, \alpha_2 = 2.5, \alpha_3 = 4.125, \alpha_4 = 5.8125, \alpha_5 = 7.39375 \text{ etc.}$$

Since $2l - 1 \leq p_l$, we can already show, by induction on l, the following statement:

$$\alpha_l \leq 2l, \text{ for all } l \geq 1.$$

Indeed, one has $\alpha_1 = 1 \leq 2$, and if the statement is true for $l-1$, we obtain:

$$\alpha_l = 1 + \alpha_{l-1} + \frac{\alpha_{l-1}}{p_l - 1} \leq 1 + 2(l-1) + \frac{2(l-1)}{p_l - 1} \leq 2l.$$

In order to study more precisely the behaviours of $\alpha(n)$ and $\beta(n)$, we will extensively use a classical lower bound for the l-th prime number, proved by Rosser in [26], and which is the following:

$$l \log l \leq p_l \text{ for all } l \geq 1.$$

We can now prove Lemma 5.1, which gives accurate upper bounds for the sequences $(\alpha_l)_{l\geq 1}$ and $(\gamma_l)_{l\geq 1}$, and Lemma 5.2, which states on the one hand that α_l and β_l are both equivalent to l when l tends to infinity, and on the other hand that when $\omega(n) = l$ is fixed, then both $\alpha(n)$ and $\beta(n)$ tends to l when $P^-(n)$ tends to infinity.

Lemma 5.1. — *The following statements hold:*

(*i*) *For every integer $n \in \mathbb{N}^*$, with $\omega(n) = l$, we have:*

$$\beta_l \leq \beta(n) \leq \alpha(n) \leq \alpha_l.$$

(*ii*) *For every integer $l \geq 1$, we have:*

$$l \leq \alpha_l \leq \frac{\alpha_9}{9} l, \ \textit{where}\ \frac{\alpha_9}{9} = \frac{166822111}{109486080} \approx 1.5237.$$

(*iii*) *For every integer $l \geq 1$, we have:*

$$\frac{5}{2} l \leq \gamma_l \leq \frac{\gamma_8}{8} l, \ \textit{where}\ \frac{\gamma_8}{8} = \frac{1784073894563}{476759162880} \approx 3.7421.$$

Proof. — (*i*) Let $n = q_1^{m_1} \dots q_l^{m_l}$ be an integer with $q_1 < \cdots < q_l$. Since for all $i \in [\![1, l]\!]$, one has $p_i \leq q_i$, we obtain the first inequality:

$$\beta_l = l - \sum_{i=1}^{l} \frac{1}{p_i} \leq l - \sum_{i=1}^{l} \frac{1}{q_i} = \beta(n).$$

The second inequality follows directly from:

$$\beta(n) = \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{P^-(d) - 1}{d} \leq \sum_{d \in \mathcal{D}_n} \frac{P^-(d) - 1}{d} = \alpha(n).$$

We prove the third inequality by induction on the number of distinct prime divisors $\omega(n) = l$ of n. For $l = 1$, the integer n is of the form $q_1^{m_1}$ and we obtain:

$$\alpha(q_1^{m_1}) = \sum_{i=1}^{m_1} \frac{q_1 - 1}{q_1^i} = \frac{q_1^{m_1} - 1}{q_1^{m_1}} \leq 1 = \alpha_1.$$

Assume now that the statement is valid for $l-1$. Therefore, we have:

$$\begin{aligned}
\alpha(q_1^{m_1}\dots q_l^{m_l}) &= \frac{q_l^{m_l}-1}{q_l^{m_l}} + \left(\sum_{i=0}^{m_l}\frac{1}{q_l^i}\right)\alpha(q_1^{m_1}\dots q_{l-1}^{m_{l-1}}) \\
&\le \frac{q_l^{m_l}-1}{q_l^{m_l}} + \left(\sum_{i=0}^{m_l}\frac{1}{q_l^i}\right)\alpha_{l-1} \\
&\le 1 + \left(\sum_{i=0}^{+\infty}\frac{1}{p_l^i}\right)\alpha_{l-1} \\
&= 1 + \frac{p_l}{p_l-1}\alpha_{l-1} = \alpha_l,
\end{aligned}$$

which proves the result.

(ii) To start with, it is straightforward that the first inequality $l \le \alpha_l$ always holds. Concerning the second inequality, one has the following:

$$\alpha_{l+1} - \alpha_l = 1 + \frac{\alpha_l}{p_{l+1}-1} \text{ for all } l \ge 1,$$

from which we deduce the two following relations:

$$\alpha_l = \alpha_1 + \sum_{k=1}^{l-1}(\alpha_{k+1}-\alpha_k) = l + \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1},$$

as well as

$$\frac{\alpha_{l+1}}{l+1} - \frac{\alpha_l}{l} \;=\; \frac{1}{l+1} + \alpha_l\left(\frac{1}{l+1}\left(1+\frac{1}{p_{l+1}-1}\right) - \frac{1}{l}\right).$$

In the remainder of this proof, we will set $\varepsilon(l) = \alpha_l - l = \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1}$, for all $l \ge 1$.

Using this notation, we obtain the following:

$$\begin{aligned}
\frac{\alpha_l}{l} - \frac{\alpha_9}{9} &= \sum_{k=9}^{l-1}\frac{1}{k+1} + \sum_{k=9}^{l-1}\alpha_k\left(\frac{1}{k+1}\left(1+\frac{1}{p_{k+1}-1}\right) - \frac{1}{k}\right) \\
&= \sum_{k=9}^{l-1}\frac{1}{k+1} - \sum_{k=9}^{l-1}\frac{k+\varepsilon(k)}{k(k+1)} + \sum_{k=9}^{l-1}\frac{\alpha_k}{(p_{k+1}-1)(k+1)} \\
&= \sum_{k=9}^{l-1}\frac{1}{k+1}\left(\frac{\alpha_k}{(p_{k+1}-1)} - \frac{\varepsilon(k)}{k}\right) \\
&= \sum_{k=9}^{l-1}\left(\frac{\varepsilon(k+1)}{k+1} - \frac{\varepsilon(k)}{k}\right) \\
&= \frac{\varepsilon(l)}{l} - \frac{\varepsilon(9)}{9}.
\end{aligned}$$

Moreover, using Rosser's lower bound, we obtain for all $l \ge 2$:

$$\varepsilon(l) = \sum_{k=1}^{l-1}\frac{\alpha_k}{p_{k+1}-1} \le \sum_{k=1}^{l-1}\frac{2k}{(k+1)\log(k+1)-1} \le 7 + \int_2^l \frac{2\mathrm{d}t}{\log t} = lf(l),$$

where we set for all $x \in \mathbb{R}$, $x \geq 2$:

$$f(x) = \frac{1}{x}\left(7 + \int_2^x \frac{2\mathrm{d}t}{\log t}\right).$$

It is readily seen that this function is non-increasing. Moreover, since:

$$\frac{\varepsilon(9)}{9} = \left(\frac{\alpha_9 - 9}{9}\right) > \frac{1}{2},$$

and since $f(l) \leq 1/2$ for all $l \geq 241$, we obtain:

$$\frac{\alpha_l}{l} \leq \frac{\alpha_9}{9}, \text{ for all } l \geq 241.$$

On the other hand, an easy computation allows us to verify that $\alpha_9/9$ is also the maximum value taken by $(\alpha_l/l)_{l\geq 1}$ on $1 \leq l \leq 240$, which proves the desired result.

(*iii*) The fact that the first inequality $5l/2 \leq \gamma_l$ always holds is straightforward. Moreover, for all $l \geq 1$, one has the following equality:

$$\begin{aligned} \gamma_{l+1} &= 3\alpha_{l+1} - \beta_{l+1} \\ &= 3 + 3\alpha_l + \frac{3\alpha_l}{p_{l+1} - 1} - \beta_l - 1 + \frac{1}{p_{l+1}} \\ &= 2 + \gamma_l + \frac{3\alpha_l}{p_{l+1} - 1} + \frac{1}{p_{l+1}}. \end{aligned}$$

Using the inequalities $5l/2 \leq \gamma_l$ and $\alpha_l \leq \alpha_9 l/9$, one can deduce that:

$$\begin{aligned} \frac{\gamma_{l+1}}{l+1} - \frac{\gamma_l}{l} &= \frac{2}{l+1} + \gamma_l\left(\frac{1}{l+1} - \frac{1}{l}\right) + \frac{3\alpha_l}{(l+1)(p_{l+1} - 1)} + \frac{1}{p_{l+1}(l+1)} \\ &\leq \frac{1}{p_{l+1}(l+1)}\left(-\frac{p_{l+1}}{2} + \frac{\alpha_9 l}{3}\left(1 + \frac{1}{p_{l+1} - 1}\right) + 1\right). \end{aligned}$$

We set, for all $x \in \mathbb{R}$, $x \geq 1$:

$$g(x) = -\frac{(x+1)\log(x+1)}{2} + \frac{\alpha_9 x}{3}\left(1 + \frac{1}{(x+1)\log(x+1) - 1}\right) + 1.$$

It is easily seen that this function is non-increasing. Moreover, since a study of g shows that $g(l) \leq 0$ for all $l \geq 9333$, we obtain:

$$\frac{\gamma_{l+1}}{l+1} - \frac{\gamma_l}{l} \leq 0, \text{ for all } l \geq 9333.$$

On the other hand, an easy computation allows us to verify that $(\gamma_l)_{l\geq 1}$ is increasing from $l = 1$ to $l = 8$ and decreasing from $l = 8$ to $l = 9333$, which proves the desired result.

$\square$

Lemma 5.2. — *The two following statements hold:*

(*i*)

$$\lim_{l\to+\infty} \frac{\alpha_l}{l} = 1 \quad \textit{and} \quad \lim_{l\to+\infty} \frac{\beta_l}{l} = 1,$$

(ii)

$$\lim_{\substack{P^-(n)\to+\infty\\ \omega(n)=l}} \alpha(n) = l \qquad \textit{and} \qquad \lim_{\substack{P^-(n)\to+\infty\\ \omega(n)=l}} \beta(n) = l.$$

Proof. — (i) Firstly, for all $l \geq 1$, one has the following inequality:

$$l \leq \alpha_l \leq l + \sum_{k=1}^{l-1} \frac{2k}{p_{k+1}-1},$$

and since the prime number theorem reads as $p_k \sim k \log k$, we can deduce that:

$$\sum_{k=1}^{l-1} \frac{k}{p_{k+1}-1} \sim \sum_{k=2}^{l} \frac{1}{\log k} \sim \frac{l}{\log l}.$$

Therefore, when l tends to infinity, we obtain $\lim\limits_{l\to+\infty} (\alpha_l/l) = 1$.

Secondly, we can deduce from Rosser's lower bound that for every $l \geq 3$, one has:

$$\begin{aligned} \beta_l &\geq l - \frac{5}{6} - \sum_{i=3}^{l} \frac{1}{i \log i} \\ &\geq l - 2 - \log\log l. \end{aligned}$$

Since, on the other hand, one always has $\beta_l \leq l$, we obtain $\lim\limits_{l\to+\infty} (\beta_l/l) = 1$, which is the desired result.

(ii) The result follows from the very definition of $\alpha(n)$ and $\beta(n)$.

□

6. Upper bounds for the little cross number

As previously stated, the upper bound implied by Theorem 2.1, and given in Corollary 2.2, is expressed as the solution of an integer linear program. Even if this formulation is more precise than any explicit formula derived from Theorem 2.1, one may still like to obtain such a formula in order to interprete the behaviour of the cross number. In the present section, we obtain such a formula in Proposition 6.1. For the proof of this result, we will use the following lemma, which can be found in [13], Proposition 5.1.11.

Lemma 6.1. — *Let H be a finite Abelian group and $G \subseteq H$ a subgroup. Then, one has:*

(i)

$$\mathsf{k}(G) + \frac{\mathsf{k}(H/G)}{\exp(G)} \leq \mathsf{k}(H).$$

(ii) *If G is a direct summand of H, then:*

$$\mathsf{k}(G) + \mathsf{k}(H/G) \leq \mathsf{k}(H).$$

We are now ready to prove the following proposition.

Proposition 6.1. — *Let G be a finite Abelian group with $r(G) = r$ and* $\exp(G) = n$. *We set $H = C_n^r$ and also:*

$$\varphi(G,H) = \begin{cases} \mathsf{k}^*(H/G) & \text{if } G \text{ is a direct summand of } H, \\ \mathsf{k}^*(H/G)/n & \text{otherwise.} \end{cases}$$

Then, one has the following upper bound for the little cross number $\mathsf{k}(G)$*:*

$$\mathsf{k}(G) \leq \sum_{d \in \mathcal{D}_n} \frac{\min\Big(\eta\big(C^r_{P^-(d)}\big), \mathsf{D}(C^r_d)\Big) - 1}{d} - \varphi(G,H).$$

Proof. — Since the group G can be injected in the group $H = C_n^r$, one obtains, applying Lemma 6.1, the relation $\mathsf{k}(G) + \varphi(G,H) \leq \mathsf{k}(H)$. Then, the desired result follows from Theorem 2.1 applied to H. $\square$

One can notice that for all $r \in \mathbb{N}^*$ and every $p \in \mathcal{P}$, one always has $\mathsf{D}(C_p^r) \leq \eta\big(C_p^r\big)$, by definition. Therefore, if we consider an elementary p-group with rank r, we obtain:

$$\mathsf{k}\left(C_p^r\right) \leq \sum_{d \in \mathcal{D}_p} \frac{\mathsf{D}(C_d^r) - 1}{d} = \frac{r(p-1)}{p} = \mathsf{k}^*\left(C_p^r\right).$$

Let G be a finite Abelian group with $r(G) = r$ and $\exp(G) = n$. Using Theorem 1.1, one obtains that if $r = 1$, then for all $d \in \mathcal{D}_n \backslash \mathcal{P}$, we have $\mathsf{D}(C_d) \geq \eta\big(C_{P^-(d)}\big)$. Moreover, when $r = 2$, then for all $d \in \mathcal{D}_n \backslash \mathcal{P}$, one has the following inequality:

$$\mathsf{D}(C_d^2) = 2d - 1 \geq 3P^-(d) - 2 = \eta\big(C^2_{P^-(d)}\big).$$

Yet, as soon as $r \geq 3$, and except for special types groups, it becomes more complicated to know exactly, for a given d in $\mathcal{D}_n \backslash \mathcal{P}$, what is the minimum of $\eta\big(C^r_{P^-(d)}\big)$ and $\mathsf{D}(C_d^r)$. For this reason, Theorem 2.1 and Proposition 6.1 remain, in general, really stronger than Proposition 2.6, which we are going to prove now. Even so, we will see in the next section that Proposition 2.6 implies sharp asymptotical results on the little cross number and the cross number.

Proof of Proposition 2.6. — Applying Proposition 6.1 and Theorem 1.2, we obtain the desired result in the following manner:

$$\begin{aligned} \mathsf{k}(G) + \varphi(G,H) &\leq \sum_{d \in \mathcal{D}_n} \frac{\min\Big(\eta\big(C^r_{P^-(d)}\big), \mathsf{D}(C^r_d)\Big) - 1}{d} \\ &\leq \sum_{d \in \mathcal{D}_n \cap \mathcal{P}} \frac{r(P^-(d) - 1)}{d} + \sum_{d \in \mathcal{D}_n \backslash \mathcal{P}} \frac{c_r(P^-(d) - 1)}{d} \\ &= c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n). \end{aligned}$$

$\square$

We can now prove the announced qualitative upper bound.

Proof of Proposition 2.1. — Since, by the definitions of Section 5, one always has the following straightforward inequalities:

$$\frac{\omega(n)}{2} \leq \beta(n) \quad \text{and} \quad \alpha(n) \leq 2\omega(n),$$

we can deduce, by Proposition 2.6 and the inequality $r \leq c_r$, the following relation:

$$\mathsf{k}(G) \leq c_r\big(\alpha(n) - \beta(n)\big) + r\beta(n) \leq \left(\frac{3c_r + r}{2}\right)\omega(n),$$

which gives the desired result. $\square$

According to the previous remark, and in the case of $r = 1$ or 2, $\eta\big(C^r_{P^-(d)}\big)$ and $\mathsf{D}(C^r_d)$ are known and easy to compare. Therefore, we can prove Proposition 2.2.

Proof of Proposition 2.2. — Applying Theorem 1.1, one can choose $c_1 = 1$ and $c_2 = 3$.

(i) For every $n \in \mathbb{N}^*$, one has by Proposition 2.6 and Lemma 5.1 $(i), (ii)$:

$$\mathsf{k}(C_n) \leq \alpha(n) \leq \alpha_{\omega(n)} \leq \frac{\alpha_9}{9}\omega(n),$$

which proves that one can take $d_1 = \alpha_9/9$.

(ii) For all $m, n \in \mathbb{N}^*$ with $1 < m|n$, one has by Proposition 2.6 applied to $G \simeq C_m \oplus C_n$ and Lemma 5.1 $(i), (iii)$:

$$\mathsf{k}(G) \leq 3\alpha(n) - \beta(n) - \varphi(G, C_n^2) \leq \gamma_{\omega(n)} \leq \frac{\gamma_8}{8}\omega(n),$$

which proves that one can take $d_2 = \gamma_8/8$.

$\square$

7. Asymptotical results

In the present section, we will apply the results obtained in Section 6 in order to prove that Conjecture 1.3 holds asymptotically in the two directions of Proposition 2.3 and Proposition 2.5.

Proof of Proposition 2.3. — First, we have:

$$\lim_{\substack{P^-(n_r) \to +\infty \\ C_{n_1} \oplus \cdots \oplus C_{n_r} \in \mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}^*(C_{n_1} \oplus \cdots \oplus C_{n_r}) = \sum_{i=1}^{r} l_i,$$

and since by the Chinese remainder theorem, every $C_{n_1} \oplus \cdots \oplus C_{n_r}$ in $\mathcal{E}_{(l_1,\ldots,l_r)}$ is a direct summand of $C^r_{n_r}$, we obtain using Lemma 6.1 (ii):

$$\begin{aligned} \mathsf{k}(C_{n_1} \oplus \cdots \oplus C_{n_r}) &\leq \mathsf{k}\left(C^r_{n_r}\right) - \mathsf{k}^*\left(C_{\frac{n_r}{n_{r-1}}} \oplus \cdots \oplus C_{\frac{n_r}{n_1}}\right) \\ &= \mathsf{k}\left(C^r_{n_r}\right) - \sum_{i=1}^{r-1} \mathsf{k}^*\left(C_{\frac{n_r}{n_i}}\right). \end{aligned}$$

On the one hand, we have by Lemma 5.2 (ii):

$$\limsup_{\substack{P^-(n_r)\to+\infty \\ \omega(n_r)=l_r}} \mathsf{k}(C^r_{n_r}) \leq \limsup_{\substack{P^-(n_r)\to+\infty \\ \omega(n_r)=l_r}} c_r\big(\alpha(n_r)-\beta(n_r)\big)+r\beta(n_r)=rl_r,$$

on the other hand, since for all $i \in [\![1,r]\!]$, the equality $\gcd(n_i, n_r/n_i) = 1$ implies $\omega(n_r/n_i) = \omega(n_r) - \omega(n_i)$, we also have:

$$\lim_{\substack{P^-(n_r)\to+\infty \\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \sum_{i=1}^{r-1} \mathsf{k}^*\left(C_{\frac{n_r}{n_i}}\right) = \sum_{i=1}^{r-1} \omega\left(\frac{n_r}{n_i}\right) = \sum_{i=1}^{r}(l_r-l_i).$$

Finally, we obtain:

$$\sum_{i=1}^{r} l_i \leq \liminf_{\substack{P^-(n_r)\to+\infty \\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}(C_{n_1}\oplus\cdots\oplus C_{n_r})$$

$$\leq \limsup_{\substack{P^-(n_r)\to+\infty \\ C_{n_1}\oplus\cdots\oplus C_{n_r}\in\mathcal{E}_{(l_1,\ldots,l_r)}}} \mathsf{k}(C_{n_1}\oplus\cdots\oplus C_{n_r}) \leq rl_r - \sum_{i=1}^{r}(l_r-l_i) = \sum_{i=1}^{r} l_i.$$

The corresponding statements for $\mathsf{K}(.)$ and $\mathsf{D}(.)$ are then deduced from Proposition 1.1. □

Since, as mentioned in Section 2, Proposition 2.4 is an immediate corollary of Proposition 2.3 by specifying $n_1 = \cdots = n_r$, we now prove an asymptotical result of an other type.

Proof of Proposition 2.5. — First, we have:

$$\lim_{\omega(n)\to+\infty} \frac{\mathsf{k}^*(C^r_n)}{\omega(n)} = r,$$

Moreover, by Proposition 2.6 applied to C^r_n, we obtain:

$$\frac{\mathsf{k}(C^r_n)}{\omega(n)} \leq c_r\left(\frac{\alpha(n)-\beta(n)}{\omega(n)}\right) + r\frac{\beta(n)}{\omega(n)},$$

which implies, by Lemma 5.2 (i), the following inequalities when $\omega(n)$ tends to infinity:

$$r = \lim_{\omega(n)\to+\infty} \frac{\mathsf{k}^*(C^r_n)}{\omega(n)} \leq \lim_{\omega(n)\to+\infty} \frac{\mathsf{k}(C^r_n)}{\omega(n)} \leq r.$$

The result for $\mathsf{K}(.)$ is then deduced from Proposition 1.1 (i). □

Each of the two previous asymptotical results admits a corollary which may appear more general at first sight. So as to state the first one, we will use the following notation, which recalls the one used for the sets $\mathcal{E}_{(l_1,\ldots,l_r)}$. For every $r, l \in \mathbb{N}^*$, we set:

$$\mathcal{E}_{r,l} = \{G \text{ finite Abelian group} \mid \mathrm{r}(G) = r,\ \omega(\exp(G)) = l\}.$$

With this notation, we obtain the following corollary.

Corollary 7.1. — *For all integers $r, l \in \mathbb{N}^*$ the three following statements hold:*

(*i*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \mathsf{k}(G) \leq rl,$$

(*ii*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \mathsf{K}(G) \leq rl,$$

(*iii*)

$$\limsup_{\substack{P^-(\exp(G)) \to +\infty \\ G \in \mathcal{E}_{r,l}}} \frac{\mathsf{D}(G)}{\exp(G)} \leq rl.$$

Proof. — Every G in $\mathcal{E}_{r,l}$ can be injected in the group $H \simeq C^r_{\exp(G)}$. Therefore, using Lemma 6.1, we obtain $\mathsf{k}(G) \leq \mathsf{k}(H)$ and the desired result follows from Proposition 2.4, applied to the group H. The corresponding statements for $\mathsf{K}(.)$ and $\mathsf{D}(.)$ are then deduced from Proposition 1.1. □

Corollary 7.2. — *For all integers $r \in \mathbb{N}^*$, the two following statements hold:*

(*i*)

$$\limsup_{\substack{\omega(\exp(G)) \to +\infty \\ r(G) \leq r}} \frac{\mathsf{k}(G)}{\omega(\exp(G))} \leq r,$$

(*ii*)

$$\limsup_{\substack{\omega(\exp(G)) \to +\infty \\ r(G) \leq r}} \frac{\mathsf{K}(G)}{\omega(\exp(G))} \leq r.$$

Proof. — Every G with rank $r(G) \leq r$ can be injected in the group $H \simeq C^r_{\exp(G)}$. Since we have $\mathsf{k}(G) \leq \mathsf{k}(H)$ by Lemma 6.1, the result follows from Proposition 2.5, applied to the group H. The statement for $\mathsf{K}(.)$ is then deduced from Proposition 1.1 (*i*). □

Acknowledgments

I am grateful to my Ph.D. advisor Alain Plagne for his help during the preparation of this article. I would like also to thank Wolfgang Schmid for his remarks on a preliminary version of this paper.

References

[1] N. Alon and M. Dubiner *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301-309.

[2] P. Baginski, S. T. Chapman, K. McDonald and L. Pudwell *On cross numbers of minimal zero sequences in certain cyclic groups*, Ars Combin. **70** (2004), 47-60.

[3] S. T. Chapman *On the Davenport constant, the cross number, and their application in factorization theory*, Zero-dimensional commutative rings (Knoxville, TN, 1994), Lecture Notes in Pure and Appl. Math., Dekker, New-York **171** (1995), 167-190.

[4] S. T. Chapman and A. Geroldinger *On cross numbers of minimal zero sequences*, Australas. J. Combin. **14** (1996), 85-92.

[5] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math. **58** (2007), 159-186.

[6] S. Elledge and G. H. Hurlbert *An application of graph pebbling to zero-sum sequences in abelian groups*, Integers **5** (2005), #A17.

[7] P. van Emde Boas *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam (1969).

[8] W. Gao and A. Geroldinger *Systems of sets of lengths II*, Abh. Math. Sem. Univ. Hamburg **70** (2000), 31-49.

[9] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337-369.

[10] W. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai *On short zero-sum subsequences II*, Integers **7** (2007), #A21.

[11] A. Geroldinger *On a conjecture of Kleitman and Lemke*, J. Number Theory **44** (1993), 60-65.

[12] A. Geroldinger *The cross number of finite abelian groups*, J. Number Theory **48** (1994), 219-223.

[13] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[14] A. Geroldinger and F. Halter-Koch *Non-unique factorizations: a survey*, Multiplicative ideal theory in commutative algebra, Springer, New York (2006), 207-226.

[15] A. Geroldinger and Y. Hamidoune *Zero-sumfree sequences in cyclic groups and some arithmetical application*, J. Théor. Nombres Bordeaux **14** (2002), 221-239.

[16] A. Geroldinger and R. Schneider *The cross number of finite abelian groups II*, European J. Combin. **15** (1994), 399-405.

[17] A. Geroldinger and R. Schneider *The cross number of finite abelian groups III*, Discrete Math. **150** (1996), 123-130.

[18] A. Geroldinger and R. Schneider *On minimal zero sequences with large cross number*, Ars Combin. **46** (1997), 297-303.

[19] U. Krause *A characterization of algebraic number fields with cyclic class group of prime power order*, Math. Z. **186** (1984), 143-148.

[20] U. Krause and C. Zahlten *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg **12** (1991), 681-696.

[21] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[22] J. E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.

[23] A. Plagne and W. A. Schmid *On large half-factorial sets in elementary p-groups: maximal cardinality and structural characterization*, Israel J. Math. **145** (2005), 285-310.

[24] A. Plagne and W. A. Schmid *On the maximal cardinality of half-factorial sets in cyclic groups*, Math. Ann. **333** (2005), 759-785.

[25] M. Radziejewski and W. A. Schmid *Weakly half-factorial sets in finite abelian groups*, Forum Math. **19** (2007), 727-747.

[26] J.B. Rosser *The n-th prime is greater than $n \log n$*, Proc. London Math. Soc. (2) **45** (1939), 21-44.

[27] P. Samuel *Théorie algébrique des nombres*, Hermann (2003).

[28] W. A. Schmid *Differences in sets of lengths of Krull monoids with finite class group*, J. Théor. Nombres Bordeaux **17**(1) (2005), 323-345.

[29] A. Schrijver *Theory of linear and integer programming*, Wiley (1998).

[30] G. Tenenbaum *Introduction à la théorie analytique et probabiliste des nombres*, Cours spécialisés, SMF (1995).

Benjamin Girard, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France. • *E-mail :* benjamin.girard@math.polytechnique.fr